

CHALLENGES OF HUMAN RIGHTS PROTECTION AND SECURITY IN THE AGE OF ARTIFICIAL INTELLIGENCE

Aleksandar S. ĐORĐEVIĆ¹

Institute of Comparative Law, Terazije 41, 11000 Belgrade

Stevica DEĐANSKI²

Faculty of Social Sciences, FNP, Belgrade, Serbia

Boris JEVTIĆ³

School of Computing, RAF, Union University Belgrade, Serbia

Abstract: *Human rights protection and security are fields in which various institutional, organizational, and humanitarian actors are involved, and their effectiveness requires continuous innovation in theory and practice. In this context, this study addresses the challenges presented by the era of artificial intelligence, aiming to improve the quality of work, collaboration, and experiences of all participants in the process of human rights and security protection supported by AI technologies. The research is based on the views of 330 respondents from the Republic of Serbia, who expressed their satisfaction with the use of modern technology tools, including the latest AI solutions, through an online survey. The survey focused on matters related to the protection of human and workers' rights, as well as communication with the media, courts,*

1 djordjevic@gmail.com

2 dedjanskis@gmail.com

3 boris.jevtic10@gmail.com

companies, and public institutions. The results, analyzed through a chi-square test from a demographic perspective, indicate significant statistical differences in satisfaction levels among respondents with higher education regarding the current state of human rights protection and the actions of organizations supported by new technologies. These findings emphasize the importance of digital education for participants and organizations in the human rights and security protection process, while also warning of potential risks associated with solutions based on a lack of algorithmic transparency, cybersecurity vulnerabilities, unfairness, bias, discrimination, negative impacts on the workforce, privacy threats, and unclear accountability for possible harm. This paper contributes to the literature and future analyses, with a focus on improving decision-makers' interactions in the human rights and security protection process. It provides an impetus for greater investment in artificial intelligence and the enhancement of knowledge and skills among all stakeholders to ensure better communication, transparency, and fair solutions that guarantee the highest level of human rights and security protection.

Keywords: *Human rights protection and security, artificial intelligence, algorithmic transparency, human control, effective legislation.*

1. INTRODUCTION

Artificial Intelligence (AI) encompasses systems that exhibit intelligent behaviour by analyzing the environment and taking actions, with a certain degree of autonomy, to achieve specific objectives in a given area of application (European Commission, 2018b). AI already holds invaluable value for the global economy and is applied across various sectors of society, including regulatory and legal spheres, daily life, psychology for a better understanding of processes like memory, linguistics, and biology, as well as for learning and mastering foreign languages from a new perspective (Čurčić, Grubor, and Jevtić, 2024; Jevtić et al., 2013). These technologies contribute to creativity, the improvement

of public, business, and media services, enhanced security and quality of life, and the resolution of complex human rights protection issues. However, they also pose challenges regarding human autonomy, privacy, and fundamental rights and freedoms (OECD, 2019; Srebro et al., 2024; Špiler et al., 2023).

The integration of artificial intelligence with other technologies, including robots equipped with AI systems, is becoming increasingly significant in communication among judicial authorities, public institutions, and the economic sector, thereby enhancing the effectiveness of human rights, security, and transparency protection. Human rights protection in the context of AI-related technologies has become a notable topic in the literature (Eliot, 2022). This technology offers numerous economic and social benefits, including the capability for extensive data collection, information security, and decision-making through algorithms. However, there is concern that AI could exacerbate economic inequalities, manipulate democratic processes, and have harmful consequences for individuals and communities, threatening human rights and legitimate expectations (Mantelero and Esposito, 2021).

Technical solutions, guidelines from professional associations, standards, and regulatory mechanisms largely respond to these challenges, while media attention and public interest also play crucial roles (European Commission, 2021). The challenge posed by artificial intelligence is its scope and complexity (Russell and Norvig, 2016), as its impact is broad and present in many aspects (Makridakis, 2017).

Given these challenges, complex and multidimensional decisions based on a detailed understanding of the issues are necessary. Although various approaches are present, such as digital education, investigative journalism, and the exchange of best practices, specificity in content related to artificial intelligence is essential. This particularly pertains to numerous difficulties in the more effective implementation and practice of international human rights standards concerning AI, which can be summarized as follows:

- Lack of a comprehensive, human rights-based approach: Sector-specific approaches are more commonly adopted when applying human rights standards, focusing on certain aspects like privacy rights, while consistent application of existing safeguards across all sectors utilizing AI is rarer. Legal frameworks, where they exist, are often not implemented effectively or promptly. Additionally, reliance on large AI platforms complicates regulatory enforcement, and oversight remains fragmented.
- Insufficient transparency and information sharing: Clear and up-to-date information on AI and its potential impact on human rights is still scarce. Intellectual property protections create barriers to enforcing the right to information – including within the judiciary, national human rights frameworks, and regulatory authorities – thereby hindering independent oversight.
- Lack of proactive initiatives by member states to utilize AI to strengthen human rights: Since the majority of AI development is driven by the private sector, public authorities are less likely to adopt a proactive approach.
- Lack of algorithmic transparency, cybersecurity vulnerabilities, and threats to privacy and data protection: These issues further complicate the effective implementation of international human rights standards in the context of AI.

In this context, the role of national human rights frameworks in ensuring human rights protection through the design, development, and implementation of AI systems, as well as in strengthening independent institutional oversight, is extremely important. Promoting transparency regarding AI systems and raising public awareness about their impact on human rights, as well as adopting a proactive approach to researching AI's potential to enhance rather than undermine human rights protection, are key goals of the research presented in

this paper. Human rights and privacy protection are regulated by international and national laws, yet there is a continuous need for improving these regulations, particularly in light of new technologies like artificial intelligence. Research into literature and practice that would allow for a better understanding of these technologies' benefits, while identifying problems and vulnerabilities related to these issues, is necessary. This paper, in this regard, aims to contribute information on the perspectives of individuals as citizens, workers, and rights holders on the importance of implementing AI in decision-making processes, communicating with decision-makers, and drafting regulations and solutions for human rights and security protection, from a demographic perspective.

The paper is structured as follows: after the introduction and theoretical framework of the research, it presents the results of the empirical study, conclusions, and references used in the elaboration of the stated views.

2. THEORETICAL FRAMEWORK

United Nations, OECD, Council of Europe, European Parliament, and European Commission documents, as well as institutions such as CEPEJ and the European Data Protection Supervisor, address issues of human rights, privacy, and their protection in the context of artificial intelligence. Academic communities and civil society organizations like *Access Now* and *Privacy International* tackle the legal challenges that AI brings, including legal personhood, intellectual property, algorithmic bias, discrimination, unfairness, labour protection, privacy, data protection, and cybersecurity. The international scope of issues related to human rights, their protection, and privacy is evident in the resolutions of the United Nations (2019), OECD (2019), Council of Europe (2017, 2018, 2019), European Parliament (2017, 2018a, 2018b, 2019, 2020a, 2020b, 2020c), European Commission (2018a, 2018b, 2020), the European Commission for the Efficiency of Justice (CEPEJ) (2018), and the European Data Protection Supervisor (2016). These resolutions cover issues such as legal personhood, intellectual property

(Schenberger, 2018), algorithmic bias, discrimination, unfairness, labour protection, privacy, data protection (Wachter and Mittelstadt, 2019), security, access to justice (Raymond, 2013), algorithmic transparency, liability for harm, accountability, and oversight. Media coverage of legal issues related to artificial intelligence technologies is increasingly prevalent and specifically addresses aspects like responsibility (Mitchell, 2019), fairness in decision-making (Niiler, 2019), bias (Marr, 2019), privacy, accountability (Coldewey, 2018), privacy, and data protection issues (Meier, 2018; Williams, 2019; Lohr, 2019). Media outlets are reporting more frequently on these topics, covering aspects like accountability, fairness in decision-making, bias, and privacy protection.

Human rights and security protection in the application of artificial intelligence (AI) face significant challenges, including a lack of algorithmic transparency. This often means that it is unclear how algorithms make decisions that affect people's rights, such as denying employment, credit, or benefits, or placing individuals on no-fly lists (Cath, 2018; Desai and Kroll, 2017). The limited availability of information on algorithm functionality (Mittelstadt et al., 2016) further complicates the situation. Analyses of social, technical, and regulatory challenges highlight the need to raise awareness and strengthen oversight and accountability in algorithmic decision-making, especially in the public sector. Solutions such as algorithmic impact assessments (Reisman et al., 2018) are promising but remain in the early stages of development, and their effectiveness has yet to be fully evaluated. Transparency in communication among judicial authorities, social organizations, private companies, and the media regarding human rights and security protection also has limitations (Anani and Kraford, 2018). Cybersecurity vulnerabilities are another critical issue in the application of AI. Velser and colleagues (2017) emphasize that automated decision-making and the use of AI without human intervention increase the risk of cybersecurity attacks. The use of AI for surveillance and cybersecurity opens up new avenues for attacks, while advanced methods of targeting political messages through social media continue to evolve. Additionally, predictive policing algorithms may negatively impact citizens' fundamental

rights (Couchman, 2019). These issues pose a threat to critical infrastructure, which can have serious consequences for society and individuals, including endangering lives and access to resources. Various strategies are employed to address these issues, such as strengthening protection, implementing recovery mechanisms, involving human analysts in critical decision-making processes, risk management programs, and software upgrades (Fralick, 2019).

Deficiencies and challenges in the field of cybersecurity require the proactive and responsible use of policies, mechanisms, and tools by developers and users alike, at all stages – from design to implementation and use. When designing systems that utilize machine learning models, engineers must carefully choose architectures, consider potential attacks, and make thoughtful compromises between model complexity, explainability, and robustness (Patel et al., 2019). This balance between security and functionality is crucial for effectively addressing these challenges. Unfairness (Smit, 2017), bias (Courtland, 2018), and discrimination (Smit, 2017) often arise as problems associated with the use of algorithms and automated decision-making systems in areas like employment, credit, criminal justice (Berk, 2019), and insurance. The European Parliament report (2017) warns that algorithms used to analyze big data can lead to violations of individuals' fundamental rights and indirect discrimination against groups with similar characteristics. This can affect fairness and equal access to education and employment, as well as the evaluation of social media users. The European Parliament has called on the European Commission, member states, and data protection authorities to identify and implement measures to reduce algorithmic discrimination and bias, as well as to develop an ethical framework for transparent data processing and automated decision-making.

Various strategies have been proposed to address these issues, including regular assessments of data representativeness and algorithm adjustments to reduce bias (Danks and London, 2017). Additionally, involving humans in the decision-making process can help (Berendt, 2019), as can opening up algorithms to enable scrutiny for bias. Standards like IEEE P7003, which are being developed as part of a global initiative for ethical autonomous systems,

provide a framework for the development of algorithmic systems that avoid unjust bias. Open-source tools, such as the *AI Fairness 360 Open Source Toolkit*, enable analysis, reporting, and reduction of bias in machine learning models using advanced algorithms and metrics. To make algorithmic auditing effective, holistic, interdisciplinary approaches based on scientific and ethical foundations are necessary (Raji and Buolamwini, 2019). There are calls for greater regulatory, political, and ethical attention to fairness, particularly in protecting vulnerable and marginalized groups.

3. METHODOLOGY

3.1 Description of the study

The empirical study conducted for this paper is based on the views of 330 respondents from the Republic of Serbia during the first half of 2024. These respondents participated in an online survey, expressing their satisfaction with the use of modern technology tools, including the latest artificial intelligence solutions, concerning the protection of human and workers' rights, as well as communication with the media, courts, companies, and public institutions.

The results, analyzed through the chi-square test from a demographic perspective, indicate significant statistical differences in satisfaction levels among respondents with higher and tertiary education concerning the current state of human rights protection and the actions of organizations engaged in the human rights and security protection process in Serbia supported by new technologies. These findings highlight the importance of digital education for participants and organizations in the rights and security protection process, while also cautioning about potential risks. These risks pertain to solutions based on a lack of algorithmic transparency, cybersecurity vulnerabilities, unfairness, bias, discrimination, negative impacts on the workforce, privacy threats, and unclear accountability for possible harm. This paper contributes to the literature and future analyses, emphasizing the improvement of decision-makers' interactions in the human rights and security protection process. It encourages greater investment in

artificial intelligence and the enhancement of knowledge and skills among all actors to ensure better communication, transparency, and the delivery of fair solutions that guarantee the highest level of rights and security protection for people.

Respondents expressed their views using a three-level satisfaction scale – dissatisfied, partially satisfied, and satisfied – on statements about the availability and timeliness of information regarding regulatory measures and legislation in this area, the public system for data use permits, reporting and monitoring mechanisms for enforcement solutions, algorithm use, analytical systems for fairness assessments, complaint mechanisms, investigative journalism, as well as stakeholder dialogue and compliance with standards in the area of human rights protection.

Table 1 shows the frequencies and percentage representation of the respondents' profile elements.

Table 1: Descriptive statistics

Gender of respondents	N	%
Male	180	54.55
Female	150	45.45
Total	330	100.00
Age group	N	%
(18–29)	46	13.94
(30–45)	127	38.48
(46–60)	73	22.12
(>60)	84	25.45
Total	330	100.00
Education level	N	%
Secondary education	137	41.52
Higher or tertiary education	193	58.48
Total	330	100,00

In the empirical study, 54.55% of the total participants were male. The largest age groups were 30–45 years old and those over 60. Respondents with higher and tertiary education represented the majority, accounting for 58.48% of the sample structure.

In this research, the chi-square test method was used. Three main and three auxiliary alternative hypotheses were defined to analyze the demographic aspects of respondents' attitudes.

The hypotheses are as follows:

- H_{01} : There are no statistically significant differences between the categories of respondents' gender in terms of satisfaction with AI technologies used in human rights and security protection.
- H_{a1} : There are statistically significant differences between the categories of respondents' gender in terms of satisfaction with AI technologies used in human rights and security protection.
- H_{02} : There are no statistically significant differences between age groups of respondents in terms of satisfaction with AI technologies used in human rights and security protection.
- H_{a2} : There are statistically significant differences between age groups of respondents in terms of satisfaction with AI technologies used in human rights and security protection.
- H_{03} : There are no statistically significant differences between the education levels of respondents in terms of satisfaction with AI technologies used in human rights and security protection.
- H_{a3} : There are statistically significant differences between the education levels of respondents in terms of satisfaction with AI technologies used in human rights and security protection.

3.2 Results

Table 2 shows the contingency table with frequencies and percentages for the gender of respondents and their satisfaction with AI technologies used in human rights and security protection.

Table 2: Contingency table for gender and satisfaction with AI technologies in human rights and security protection

Frequency Overall % Column % Row %	Dissatisfied	Partially satisfied	Satisfied	Total
Male	40	78	62	180
	12.12	23.64	18.79	
	47.62	54.93	59.62	
	22.22	43.33	34.44	
Female	44	64	42	150
	13.33	19.39	12.73	
	52.38	45.07	40.38	
	29.33	42.67	28.00	
Total	84	142	104	330
	25.45	43.03	31.52	

Table 3 provides contingency frequencies, overall percentages, and breakdowns by column and row for respondents’ age groups in relation to their satisfaction with AI technologies used in human rights and security protection.

Table 3: Contingencies for age groups of respondents in relation to satisfaction with AI technologies in human rights and security protection

Frequency Overall % Column % Row %	Dissatisfied	Partially satisfied	Satisfied	Total
(18–45)	40	78	55	173
	12.12	23.64	16.67	
	47.62	54.93	52.88	
	23.12	45.09	31.79	
>45	44	64	49	157
	13.33	19.39	14.85	
	52.38	45.07	47.12	
	28.03	40.76	31.21	
Total	84	142	104	330
	25.45	43.03	31.52	

Table 4 provides contingency frequencies, overall percentages, and breakdowns by column and row for respondents' education levels in relation to their satisfaction with AI technologies used in human rights and security protection.

Table 4: Contingencies for education levels of respondents in relation to satisfaction with AI technologies in human rights and security protection

Frequency Overall % Column % Row %	Dissatisfied	Partially satisfied	Satisfied	Total
Secondary education	40 12.12 47.62 29.20	65 19.70 45.77 47.45	32 9.70 30.77 23.36	137
Higher or tertiary education	44 13.33 52.38 22.80	77 23.33 54.23 39.90	72 21.82 69.23 37.31	193
Total	84 25.45	142 43.03	104 31.52	330

Table 5 provides the observed and theoretical chi-square test values and statistical significances according to gender, age, and education level of respondents in relation to satisfaction with AI technologies in human rights and security protection.

Table 5: Observed and theoretical chi-square test values with statistical significance

Gender of respondents / Satisfaction with AI technologies in human rights and security protection						
Test	Chi-Square (observed)	Statistical significance (observed)	df	Chi-Square (theoretical)	Statistical significance (theoretical)	H ₀₁
Value	2.712	0.2577	2	5.991	0.05	Accept
Age of respondents / Satisfaction with AI technologies in human rights and security protection						
Test	Chi-Square (observed)	Statistical significance (observed)	df	Chi-Square (theoretical)	Statistical significance (theoretical)	H ₀₂
Value	1.144	0.5644	2	5.991	0.05	Accept
Education level of respondents / Satisfaction with AI technologies in human rights and security protection						
Test	Chi-Square (observed)	Statistical significance (observed)	df	Chi-Square (theoretical))	Statistical significance (theoretical)	H ₀₄
Value	7.296	0.0260	2	5.991	0.05	Reject

Based on the data from Table 5, the following conclusions can be drawn:

- H_{01} : There are no statistically significant differences among gender categories in satisfaction with AI technologies used in human rights and security protection.
- H_{a1} : There are statistically significant differences among gender categories in satisfaction with AI technologies used in human rights and security protection.

The significance threshold is 0.05, with a degree of freedom of 2 and a critical χ^2 value of 5.991. The observed χ^2 value of 2.712 is less than the table value of 5.991, and the observed p-value of 0.2577 is greater than 0.05. Thus, the null hypothesis is accepted, meaning no statistically significant difference was observed among the gender categories of respondents regarding satisfaction with the use of AI technologies in human rights and security protection.

- H_{02} : No statistically significant difference was observed among the age categories of respondents regarding satisfaction with the use of AI technologies in human rights and security protection.
- H_{a2} : A statistically significant difference exists between the age categories of respondents regarding satisfaction with the use of AI technologies in human rights and security protection.

The significance level is 0.05, with a degree of freedom of 2 and a critical value for $\chi^2 = 5.991$. The obtained χ^2 value of 1.144 is less than the table value of $\chi^2 = 5.991$, and the obtained p-value of 0.5644 is greater than the threshold of 0.05. Therefore, the null hypothesis is accepted, indicating that no statistically significant difference was observed among the age categories of respondents regarding satisfaction with the use of AI technologies in human rights and security protection.

- H_{03} : No statistically significant difference exists between the education level categories of respondents regarding satisfaction with the use of AI technologies in human rights and security protection.
- H_{a3} : A statistically significant difference exists between the education level categories of respondents regarding satisfaction with the use of AI technologies in human rights and security protection.

The significance level is 0.05, with a degree of freedom of 2 and a critical value for $\chi^2 = 5.991$. The obtained χ^2 value of 7.296 is greater than the table value of $\chi^2 = 5.991$, and the obtained p-value of 0.0260 is less than the threshold of 0.05. Therefore, the null hypothesis is rejected, and the alternative hypothesis H_{a3} is accepted, indicating that a statistically significant difference was observed among the education level categories of respondents regarding satisfaction with the use of AI technologies in human rights and security protection (Jevtić et al., 2024).

4. CONCLUSION

This paper provides an overview of the literature on various legal issues and challenges related to artificial intelligence (AI), including its impact on human rights (Miškić et al., 2023). The results of the study on citizens' views regarding regulatory, technological, and standardization issues of human rights protection in Serbia identify the need to improve digital literacy, particularly concerning AI, to increase the level of awareness and cooperation among all participants in the human rights and security protection process. Key actions for the protection of vulnerable social groups, which carry far-reaching social and legal implications, relate to fundamental rights such as data protection, equality, freedom, autonomy, dignity, justice, non-discrimination, and privacy. It is essential to encourage these actions through increased investments in technological infrastructure, regulatory frameworks, solutions, and the judiciary, as well as through the collaboration of all

stakeholders contributing to improving the level of protection and security in Serbia.

Notably, findings from the socio-economic research conducted as part of the SIENNA project (Jansen, 2018) further emphasize concerns regarding these issues. In addition to specific challenges, general legal issues include the lack of AI regulation in Serbia, unclear application of existing laws, and a lack of legal discourse and knowledge among judicial actors (Rodrigues, 2019). Given that AI technologies work with large volumes of data, they have multiplicative effects that further complicate legal issues and challenges in the area of human rights. The consulted literature for this paper reveals several shortcomings: at the level of policy and legislation, technical development, and in involving various stakeholders. Although some of these deficiencies have begun to be addressed, additional commitment is needed in the country. Technical deficiencies are especially significant because legal and ethical issues can be integrated into the AI system's design and development phase, which would significantly contribute to the success of AI systems.

The lack of involvement of various stakeholders poses a challenge, as their different interests (innovation, ethical compliance, profit) need to be carefully balanced. Additionally, the voices of vulnerable communities are often underrepresented. There is a need to involve a wide range of actors to consider specific vulnerabilities in different AI application contexts. As AI technologies advance, additional legal and ethical challenges will emerge, including new types of vulnerabilities that will require continuous monitoring and research. Progress in AI, robotics, and IoT will bring new dilemmas for laws in Serbia and societal values, which will require refreshed discussions and regulatory adjustments.

LITERATURE

1. Ananny, Mike, and Kate Crawford. 2018. "Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability." *New Media & Society* 20 (3): 973–989. <https://doi.org/10.1177/1461444816676645>.

2. Berk, Richard A. 2019. "Accuracy and Fairness for Juvenile Justice Risk Assessments." *Journal of Empirical Legal Studies*. https://crim.sas.upenn.edu/sites/default/files/Berk_FairJuvy_1.2.2018.pdf.
3. Berendt, Bettina. 2019. "AI for the Common Good?! Pitfalls, Challenges, and Ethics Pen-Testing." *Paladyn, Journal of Behavioral Robotics* 10: 44–65. <https://doi.org/10.1515/pjbr-2019-0004>.
4. Council of Europe. 2019. *Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights*.
5. Coldewey, Devin. 2018. "AI Desperately Needs Regulation and Public Accountability, Experts Say." *TechCrunch*, December 7. <https://techcrunch.com/2018/12/07/ai-desperately-needs-regulation-and-public-accountability-experts-say/>.
6. Cath, Corinne. 2018. "Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. <https://doi.org/10.1098/rsta.2018.0080>.
7. Courtland, Rachel. 2018. "Bias Detectives: The Researchers Striving to Make Algorithms Fair." *Nature*. <https://www.nature.com/articles/d41586-018-05469-3>.
8. Couchman, Hannah. 2019. *Policing by Machine: Predictive Policing and the Threats to Our Rights*. Liberty Human Rights. <https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf>.
9. Čurčić, Nemanja, Aleksandar Grubor, and Bojan Jevtić. 2024. "Implementing Artificial Intelligence in Travel Services: Customer Satisfaction Gap Study at Serbian Airports." *Ekonomika* 3/2024.
10. Danks, David, and Alex J. London. 2017. "Algorithmic Bias in Autonomous Systems." In *Proceedings of the 26th International Joint Conference on Artificial Intelligence*. AAAI Press. <https://www.cmu.edu/dietrich/philosophy/docs/london/IJCAI17-AlgorithmicBias->

11. Desai, Deven R., and Joshua A. Kroll. 2017. "Trust but Verify: A Guide to Algorithms and the Law." *Harvard Journal of Law & Technology* 31: 1.
12. Eliot, Lance. 2022. "Responsible AI Relishes Preeminent Boost Via AI Ethics Proclamation by Top Professional Society the ACM." *Forbes*.
13. European Parliament. 2017. "Resolution of 14 March 2017 on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law Enforcement (2016/2225(INI))."
14. European Commission. 2018a. "Coordinated Plan on Artificial Intelligence." COM (2018) 795 final, Brussels.
15. European Commission. 2021. "Proposal for a Regulation on a European Approach for Artificial Intelligence." COM(2021) 206 final.
16. European Commission. 2020. "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust." COM(2020) 65 final, Brussels.
17. Executive Office of the President. 2016. *Preparing for the Future of Artificial Intelligence*.
18. Fralick, Courtney. 2019. "Artificial Intelligence in Cybersecurity Is Vulnerable." *SC Magazine*. <https://www.scmagazine.com/home/opinion/artificial-intelligence-in-cybersecurity-is-vulnerable/>.
19. Jansen, Pieter. 2018. *SIENNA D4.1 State of the Art Review: AI and Robotics*. SIENNA Project. https://www.sienna-project.eu/digitalAssets/787/c_787382-1_1-k_sienna-d4.1-state-of-the-art-review-final-v.04.pdf.
20. Jevtić, Bojan, Stevica Dedanski, Milorad Beslać, Ratko Grozdanić, and Aleksandar Damnjanović. 2013. "SME Technology Capacity Building for Competitiveness and Export: Evidence from Balkan Countries." *Metalurgija International* 18 (special issue 4): 162–170. București: Editura Științifică F.M.R. <https://enauka.gov.rs/handle/123456789/676927>.
21. Jevtić, Bojan, Milorad Beslać, Dragana Janjušić, and Marija Jevtić. 2024. "The Effects of Digital Natives' Expectations of Tech Hotel Services

- Quality on Customer Satisfaction.” *International Journal for Quality Research* 18 (1): 1–10. <https://doi.org/10.24874/IJQR18.01-01>.
22. Lohr, Steve. 2019. “AI and Privacy Concerns Get White House to Embrace Global Cooperation.” *The New York Times*. <https://www.nytimes.com/2019/04/03/technology/artificial-intelligence-privacy-oecd.html>.
23. Mittelstadt, Brent D., Philip Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi. 2016. “The Ethics of Algorithms: Mapping the Debate.” *Big Data & Society*. <https://doi.org/10.1177/2053951716679679>.
24. Marr, Bernard. 2019. “Artificial Intelligence Has a Problem with Bias, Here’s How to Tackle It.” *Forbes*. <https://www.forbes.com/sites/bernardmarr/2019/01/29/3-steps-to-tackle-the-problem-of-bias-in-artificial-intelligence/>.
25. Mitchell, Iain. 2019. “The Use of AI Gives Rise to Huge Potential Legal Issues.” *The Scotsman*. <https://www.scotsman.com/lifestyle/iain-mitchell-the-use-of-ai-gives-rise-to-huge-potential-legal-issues-1-4924962>.
26. Makridakis, Spyros. 2017. “The Forthcoming Artificial Intelligence (AI) Revolution: Its Impact on Society and Firms.” *Futures* 90: 46–60. <https://doi.org/10.1016/j.futures.2017.03.006>.
27. Mantelero, Alessandro, and Massimo S. Esposito. 2021. “An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems.” *Computer Law & Security Review* 41: 105561. <https://doi.org/10.1016/j.clsr.2021.105561>.
28. Miškić, Milana, Bojana Srebro, Marko Rašković, Milan Vrbanc, and Bojan Jevtić. 2024. “Key Challenges Hindering SMEs’ Full Benefit from Digitalization: A Case Study from Serbia.” *International Journal for Quality Research* 19 (2). <https://doi.org/10.22874/IJQR1902-03>.
29. Niiler, Eric. 2019. “Can AI Be a Fair Judge in Court? Estonia Thinks So.” *Wired*. <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so>.

30. OECD. 2019. *Artificial Intelligence in Society*. Paris: OECD Publishing. <https://doi.org/10.1787/eedfee77-en>.
31. Patel, Anya, Themis Hatzakis, Kevin Macnish, Mark Ryan, and Anatolii Kirichenko. 2019. "Cyberthreats and Countermeasures." *SHERPA Project*. <https://doi.org/10.21253/DMU.7951292.v3>.
32. Privacy International & Article 19. 2018. *Privacy and Freedom of Expression in the Age of Artificial Intelligence*. <https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf>.
33. Raji, Inioluwa Deborah, and Joy Buolamwini. 2019. "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products." *AAAI/ACM Conference on AI Ethics and Society*.
34. Raymond, Adam H., and Scott J. Shackelford. 2013. "Technology, Ethics, and Access to Justice: Should an Algorithm Be Deciding Your Case?" *Michigan Journal of International Law* 35: 485.
35. Russell, Stuart J., and Peter Norvig. 2016. *Artificial Intelligence: A Modern Approach*. Pearson Education Limited.
36. Rodrigues, Rowena, Alexandros Panagiotopoulos, David Wright, Themis Hatzakis, and Stella Laulhé Shaelou. 2020. "SHERPA Deliverable 3.3 Report on Regulatory Options." *SHERPA Project*. <https://doi.org/10.21253/DMU.8181827.v2>.
37. Schönberger, Daniel. 2018. "Deep Copyright: Up-and-Downstream Questions Related to Artificial Intelligence (AI) and Machine Learning (ML)." *Zeitschrift für Geistiges Eigentum/Intellectual Property Journal* 10 (1): 35.
38. Srebro, Bojana, and Bojan Jevtić. 2024. "Improving Decision-Making Efficiency Through AI-Powered Fraud Detection and Prevention." *International Congress on Project Management of ICT*, Arandelovac, 2024.

39. Smith, Laura. 2017. "Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making." *Future of Privacy Forum*. <https://fpf.org/2017/12/11/unfairness-by-algorithm-distilling-the-harms-of-automated-decision-making/>.
40. United Nations. 2019. *United Nations Activities on Artificial Intelligence (AI)*. <http://handle.itu.int/11.1002/pub/813bb49e-en>.
41. Williams, Holly. 2019. "Big Brother AI Is Watching You." *IT ProPortal*. <https://www.itproportal.com/features/big-brother-ai-is-watching-you/>.
42. Wachter, Sandra, and Brent D. Mittelstadt. 2019. "A Right to Reasonable Inferences: Rethinking Data Protection Law in the Age of Big Data and AI." *Columbia Business Law Review*. https://oralex.ac.uk/objects/uuid:d53f7b6a-981c-4f87-91bc-743067d10167/download_file?file_format=pdf.